UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,088	12/11/2000	David Michael Kurn	20206-032 (P00-3016)	5327

7590 10/01/2004

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
JACK, TODD M	

ART UNIT	PAPER NUMBER
2133	

DATE MAILED: 10/01/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/735,088	KURN ET AL.	
	Examiner	Art Unit	
	Todd M Jack	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 DEC 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-69* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-69* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 1-5. 4/30/2001
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☒ Other: *Detailed Action*.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1-5, 9-12, 14-20, 28-32, 35-37, 47-50, 51-53 are rejected under 35 U.S.C. 102(e) as being anticipated by Wool (6,373,948).

Claim 1: Wool teaches a computer configuration with encrypted multimedia information (col. 4, 40-54), a head-end server (col. 5, lines 50-51), a head-end server includes a processor and related memory, as a data storage device (col. 8, lines 29-32), a set-top terminal executes a decode process to decrypt programs that a customer is entitled to, by using the received program identifier and the stored entitlement information to derive the program key and then using the program key to decrypt the program (col. 12, lines

13-18), the set-top terminal does not have access to the master key matrix but the program keys must be obtained indirectly using the customer key matrix and the received program identifier (col. 6, lines 62-67 and col. 7, lines 1-3) where the matrix is believed to be the repository and access is controlled by the identifier, the processor includes a control unit, an arithmetic logic unit and a local memory storage device where the control unit retrieves instruction from the data storage device or ROM (col. 8, lines 37-46), the head-end server will transmit the program identifier, with the encrypted program (col. 6, lines 60-62), and the program database indicates the program identifier and associated packages corresponding to each program with topic hierarchy is utilized to organize programs (col. 8, lines 47-65) to allow access by applications with authorization.

Claim 2: Further, Wool teaches the set-top terminal includes any mechanism to restrict access to the transmitted multimedia information using decryption keys (col. 4, lines 46-52).

Claim 3: Further, Wool teaches each of the k-bit program keys used to encrypt transmitted pro-grams is a linear combination of a defined set of k-bit master keys (col. 3, lines 12-16).

Claim 4: Further, Wool teaches using a received program identifier and the stored entitlement information to derive the program key and then using the program key to decrypt the program (col. 12, lines 13-18).

Claim 5: Further, Wool teaches restricting access to the transmitted multimedia information using decryption keys (col. 4, lines 48-52) where access would not have been required if the information were not a secret.

Claim 9: Further, Wool teaches the data storage device includes the master key matrix (col. 8, lines 47-48).

Claim 10: Further, Wool teaches the data storage device includes the master key matrix (col. 8, lines 47-48).

Claim 11: Further, Wool teaches the entitlement database is preferably stored in a secure portion of the data storage device (col. 9, lines 21-22).

Claim 12: Further, Wool teaches the processor includes a control unit, an arithmetic logic unit and a local memory storage device, such as, for example, an instruction cache or a plurality of registers (col. 8, lines 34-42).

Claim 13: Further, Wool teaches a master key matrix where the program key is a linear combination of the master keys. A program key is used to decrypt the received program. The program key is a linear combination of master keys. (col. 6, lines 62-67 and col. 7, lines 1-3)

Claim 14: Further, Wool teaches a set-top terminal includes any mechanism to restrict access to the transmitted multimedia information using decryption keys (col. 4, lines 48-51).

Claim 15: Wool teaches the network environment for transferring encrypted multimedia information for access is restricted to the transmitted multimedia information using decryption keys (col. 4, lines 40-48), a head-end server includes a processor and related memory, as a data storage device (col. 8, lines 29-32), a set-top terminal executes a decode process to decrypt programs that a customer is entitled to, by using the received program identifier and the stored entitlement information to derive the program key and then using the program key to decrypt the program (col. 12, lines 13-18), the head-end server will transmit the program identifier, with the encrypted program (col. 6, lines 60-62), the set-top terminal does not have access to the master key matrix but the program keys must be obtained indirectly using the customer key matrix and the received program identifier (col. 6, lines 62-67 and col. 7, lines 1-3) where the matrix is believed to be the repository and access is controlled by the identifier, the processor includes a control unit, an arithmetic logic unit and a local memory storage device where

the control unit retrieves instruction from the data storage device or ROM (col. 8, lines 37-46), and the program database indicates the program identifier and associated packages corresponding to each program with topic hierarchy is utilized to organize programs (col. 8, lines 47-65) to allow access by applications with authorization.

Claim 16: Wool teaches a computer configuration with encrypted multimedia information (col. 4, 40-54), a head-end server (col. 5, lines 50-51), a head-end server includes a processor and related memory, as a data storage device (col. 8, lines 29-32), a set-top terminal executes a decode process to decrypt programs that a customer is entitled to, by using the received program identifier and the stored entitlement information to derive the program key and then using the program key to decrypt the program (col. 12, lines 13-18), the set-top terminal does not have access to the master key matrix but the program keys must be obtained indirectly using the customer key matrix and the received program identifier (col. 6, lines 62-67 and col. 7, lines 1-3) where the matrix is believed to be the repository and access is controlled by the identifier, and the program database indicates the program identifier and associated packages corresponding to each program with topic hierarchy is utilized to organize programs (col. 8, lines 47-65) to allow access by applications with authorization.

Claim 17: Further, Wool teaches the set-top terminal includes any mechanism to restrict access to the transmitted multimedia information using decryption keys (col. 4, lines 46-52).

Claim 18: Further, Wool teaches each of the k-bit program keys used to encrypt transmitted pro-grams is a linear combination of a defined set of k-bit master keys (col. 3, lines 12-16).

Claim 19: Further, Wool teaches each of the k-bit program keys used to encrypt transmitted pro-grams is a linear combination of a defined set of k-bit master keys (col. 3, lines 12-16). This encryption protects the sensitive information; i.e. programs.

Claim 20: Further, Wool teaches using a received program identifier and the stored entitlement information to derive the program key and then using the program key to decrypt the program (col. 12, lines 13-18).

Claim 28: Further, Wool teaches the data storage device includes the master key matrix (col. 8, lines 47-48).

Claim 29: Further, Wool teaches the data storage device includes the master key matrix (col. 8, lines 47-48).

Claim 30: Further, Wool teaches the data storage device includes the master key matrix (col. 8, lines 47-48).

Claim 31: Further, Wool teaches the processor includes a control unit, an arithmetic logic unit and a local memory storage device, such as, for example, an instruction cache or a plurality of registers (col. 8, lines 34-42).

Claim 32: Wool teaches a head-end server (col. 5, lines 50-51), the head-end server will transmit the program identifier, with the encrypted program (col. 6, lines 60-62), a head-end server includes a processor and related memory, as a data storage device (col. 8, lines 29-32), a set-top terminal executes a decode process to decrypt programs that a customer is entitled to, by using the received program identifier and the stored entitlement information to derive the program key and then using the program key to decrypt the program (col. 12, lines 13-18), the set-top terminal does not have access to the master key matrix but the program keys must be obtained indirectly using the customer key matrix and the received program identifier (col. 6, lines 62-67 and col. 7, lines 1-3) where the matrix is believed to be the repository and access is controlled by the identifier, the processor includes a control unit, an arithmetic logic unit and a local memory storage device where the control unit retrieves instruction from the data storage device or ROM (col. 8, lines 37-46), once the customer obtains the program key, to each of the entitled programs, then the customer may also easily derive the program keys to 2r programs resulting in information leaking (col. 6, lines 9-19), a set-top terminal includes any mechanism to restrict access to the transmitted multimedia information using decryption keys (col. 4, lines 48-52), the program identifier which is transmitted in the ECM field defined in the MPEG-2 standard (col. 5, lines 24-31), and

each transmitted program is encrypted by the head-end server using a program key (col. 5, lines 10-12).

Claim 35: Further, Wool teaches the set-top terminal includes any mechanism to restrict access to the transmitted multimedia information using decryption keys (col. 4, lines 46-52).

Claim 36: Further, Wool teaches each of the k-bit program keys used to encrypt transmitted pro-grams is a linear combination of a defined set of k-bit master keys (col. 3, lines 12-16).

Claim 37: Further, Wool teaches using a received program identifier and the stored entitlement information to derive the program key and then using the program key to decrypt the program (col. 12, lines 13-18).

Claim 47: Further, Wool teaches the data storage device includes the master key matrix (col. 8, lines 47-48).

Claim 48: Further, Wool teaches the data storage device includes the master key matrix (col. 8, lines 47-48).

Claim 49: Further, Wool teaches the data storage device includes the master key matrix (col. 8, lines 47-48).

Claim 50: Further, Wool teaches the processor includes a control unit, an arithmetic logic unit and a local memory storage device, such as, for example, an instruction cache or a plurality of registers (col. 8, lines 34-42).

Claim 51: Further, Wool teaches the set-top terminal does not have access to the master key matrix but the program keys must be obtained indirectly using the customer key matrix and the received program identifier (col. 6, lines 62-67 and col. 7, lines 1-3) where the matrix is believed to be the repository and access is controlled by the identifier.

Claim 52: Further, Wool teaches using a received program identifier and the stored entitlement information to derive the program key and then using the program key to decrypt the program (col. 12, lines 13-18).

Claim 53: Further, Wool teaches a transmitted program is encrypted by the head-end server using a program key (col. 5, lines 10-20).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 6, 8, 21, 34, 38, 43, 56, and 63-69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wool and Levin (6,272,152).

Claim 6: Wool fails to teach sensitive information is a private key. Levin teaches a certificate has a name field to contain the name of the holder of the private key (col. 6, lines 5-9).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by a private key to protect the sensitive information. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to provide the capability to protect the system.

Claim 8: Wool fails to teach a sensitive information is a certification authority certificate. Levin teaches a certificate has a name field to contain the name of the holder of the private key (col. 6, lines 6-8).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by a certification authority certificate. This modification would have been obvious because a person

having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to insure that only authorized parties have access to the system.

Claim 21: Wool fails to teach sensitive information is a private key. Levin teaches a certificate has a name field to contain the name of the holder of the private key (col. 6, lines 5-9).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by a private key to protect the sensitive information. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to provide the capability to protect the system.

Claim 34: Wool fails to teach a key repository is constructed and arranged to record the authorization information in the database. Levin teaches that if there is any discrepancy, the decision module terminates the financial transaction and the validation server transfers the message and all succeeding messages that were stored in a buffer while the sever was validating the credit worthiness (col. 6, lines 32-40).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by having the decision module validate and store in the buffer. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to save the validation information for later use.

Claim 38: Wool fails to teach sensitive information is a private key. Levin teaches a certificate has a name field to contain the name of the holder of the private key (col. 6, lines 5-9).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by a private key to protect the sensitive information. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to provide the capability to protect the system.

Claim 43: Wool fails to teach a sensitive information is a certification authority certificate. Levin teaches a certificate has a name field to contain the name of the holder of the private key (col. 6, lines 6-8).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by a certification authority certificate. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to insure that only authorized parties have access to the system.

Claim 56: Wool fails to teach the instance of the application is recognized by its physical address. Levin teaches the current attributes of the cable user owning a terminal would be looked up using the MAC address of terminal (col. 6, lines 42-47).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by making the application is recognized by its physical address. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to easily locate the attribute.

Claim 60: Wool fails to teach the instance of the application is recognized by a packet header. Levin teaches the header of the protocol data unit is checked when the protocol data unit that is the start of a new message is sensed. (col 5, lines 25-29)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by allowing the packet header to recognize the application. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to allow a packet of information to stand alone by authorizing access to its data.

Claim 63: Wool fails to teach the instance of the application is recognized by its physical address. Levin teaches the current attributes of the cable user owning a terminal would be looked up using the MAC address of terminal (col. 6, lines 42-47).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by using addresses for the attribute. This modification would have been obvious because a person having

ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to recognize a valid application that can operate on the system.

Claim 64: Wool fails to teach authorization information includes a universal resource locator. Levin teaches the use of a URL to indicate a financial transaction (col. 6, lines 61-64).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by implementing a URL. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to identify information.

Claim 65: Wool fails to teach the authorization information includes a system residence. Levin teaches the associating the MAC address with the user identity (col. 6, lines 19-24).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by utilizing the system residence. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to authorized information.

Claim 66: Wool fails to teach the directive to authorize the application is provided by an operator. Levin teaches the user wants to conduct a financial transaction, and then the parsing module extracts the cardholder certificate (col. 6, lines 13-24).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by authorizing the application. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to seek permission to enter the system.

Claim 67: Wool fails to teach the directive to authorize the application is provided by an owner. Levin teaches the phone number is used to look up, in a database of the validation server, the identity of the user and the location of the terminal (col. 7, lines 59-64). The owner of the phone can only transmit the telephone number as they call the Internet network.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by having an owner authorize the application. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to verify the owner without additional number input.

Claim 68: Wool fails to teach the directive to authorize the application is provided by an owner. Levin teaches the phone number is used to look up, in a database of the

validation server, the identity of the user and the location of the terminal (col. 7, lines 59-64). The owners of the phone can only transmit the telephone number as they call the Internet network.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by having an owner authorize the application. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to verify the owner without additional number input.

Claim 69: Wool fails to teach the directive to authorize the application is provided by an owner. Levin teaches the phone number is used to look up, in a database of the validation server, the identity of the user and the location of the terminal (col. 7, lines 59-64). The owner of the phone can only transmit the telephone number as they call the Internet network.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool by having an owner authorize the application. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to verify the owner without additional number input.

Claims 7, 22, 27, 28, 38, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wool in view of Schneier.

Claim 7: Wool fails to teach a sensitive information is a symmetric key. Schneier teaches the security of a symmetric cryptosystem is a function of two things: the strength of the algorithm and the length of the key (chapter 7.1, par. 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to utilize a symmetric key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to enhance the security of the system.

Claim 22: Wool fails to teach a sensitive information is a symmetric key. Schneier teaches the security of a symmetric cryptosystem is a function of two things: the strength of the algorithm and the length of the key (chapter 7.1, par. 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to utilize a symmetric key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to enhance the security of the system.

Claim 27: Wool fails to teach a trust root is a cryptographic mechanism. Schneier teaches a cryptosystem is an algorithm, plus all possible plaintexts, cipher texts, and keys (p. 4, par. 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to create a trust root, which is a cryptographic mechanism. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to allow the cryptographic operations to be accessed according to a hierarchy.

Claim 28: Wool fails to teach a sensitive information is a symmetric key. Schneier teaches the security of a symmetric cryptosystem is a function of two things: the strength of the algorithm and the length of the key (chapter 7.1, par. 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to utilize a symmetric key. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to enhance the security of the system.

Claim 42: Wool fails to teach the sensitive secret is a digital signature. Schneier teaches a general digital signature scheme which is an encrypted DSA signature scheme (chapter 20.4, par. 1-2).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to use a signature, which is a secret. This modification would have been obvious because a person having

ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to ensure that the signature was accessed by unauthorized individuals and replicated.

Claims 23-24, 40-41, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wool in view of Menezes.

Claim 23: Wool fails to teach a sensitive secret is a trust root. Menezes teaches a public key of the root node (p. 573, par. 6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to have a sensitive secret as a root. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to access authorized information for the purpose of decrypting/encrypting information.

Claim 24: Wool fails to teach a trust root is a digital fingerprint. Menezes teaches compact representative image called digital fingerprint (page 321, par. 2).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to place a digital fingerprint in a trust root. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to uniquely identify the object.

Claim 40: Wool fails to teach a sensitive secret is a trust root. Menezes teaches a public key of the root node (p. 573, par. 6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to have a sensitive secret as a root. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to access authorized information for the purpose of decrypting/encrypting information.

Claim 41: Wool fails to teach a trust root is a digital fingerprint. Menezes teaches compact representative image called digital fingerprint (page 321, par. 2).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to place a digital fingerprint in a trust root. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to uniquely identify the object.

Claim 46: Wool fails to teach that sensitive secrets are a characteristic code sequence. Menezes teach that cryptographic codes operate on units such as words, groups of words, or phrases and substitute these by designated words, letter groups, or number groups called code groups.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to include sensitive secrets are a characteristic code sequence. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to transport the codes in a secure encrypted manner.

Claims 25, 44, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wool in view of that which is commonly known in the art.

Claim 25: Wool fails to teach a trust root is a checksum. It is commonly known to one knowledgeable in the art to modify the invention of Wool by making a trust root, which is the checksum in order that a total of the financial transactions may occur.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to place a checksum in a root directory. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to total financial transactions.

Claim 44: Wool fails to teach a sensitive secret is a checksum. It is commonly known to one knowledgeable in the art to modify the invention of Wool by making a trust root, which is the checksum in order that a total of the financial transactions.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to place a checksum in a root directory. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to total financial transactions and allow only authorized individuals access to the total value.

Claim 54: Wool fails to teach a sensitive secret is a checksum. It is commonly known to one knowledgeable in the art to modify the invention of Wool by making a trust root, which is the checksum in order that a total of the financial transactions.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to place a checksum in a root directory. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to total financial transactions and allow only authorized individuals access to the total value.

Claims 26 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wool in view of Schneier, further in view of that which is commonly known in the art.

Claim 26: Wool fails to teach the trust root is a hash. Schneier teaches a hash value (chapter 2.4). It is commonly known in the art that the hash can be a root in order to access it in a processor hierarchy.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to include a root, which is a hash. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to be able to access the hash function in a processor hierarchy for the data can be encrypted.

Claim 45: Wool fails to teach the trust root is a hash. Schneier teaches a hash value (chapter 2.4). It is commonly known in the art that the hash can be a root in order to access it in a processor hierarchy.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to include a root, which is a hash. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to be able to access the hash function in a processor hierarchy for the data can be encrypted.

Claim 33, 57-59, and 61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wool in view of Denning (Cryptography and Data Security, 1982).

Claim 33: Wool fails to teach directing the key repository to recognize instances of the application. Denning teaches the operating system can freely move segments main and secondary memory merely by updating the descriptors and a program is affected by relocations of segments in the memory hierarchy (page 232, column 1, paragraph 1, and column 2, paragraph 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to recognize instances of the application. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to recognize and utilize a specific instance, which is in need.

Claim 57: Wool fails to teach the instance of the application is recognized by the system on which it is instantiated. Denning teaches algorithms for computing ciphertext (page 161, paragraph 7) where the cipher text must be a recognized item in order to be implemented.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to where the cipher must be recognized to use the cipher to encrypt the code. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to authenticate the application.

Claim 58: Wool fails to teach an instance of the application is recognized by the nature of the interconnection to the key repository. Denning teaches a private key on some digital storage medium which can be inserted into A's terminal, and that a copy of the key is stored on file at the system (page 162, paragraph 6).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to include the recognition of the interconnection to the key repository. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to determine which instance belongs to a particular process.

Claim 59: Wool fails to teach the instance of the application is recognized by its communication protocol. Denning teaches communication protocols for initiating and terminating connections and synchronizing key streams (page 138, page 1).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to include communication protocol recognition. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Denning, in order to determine the compatibility of the applications.

Claim 61: Wool fails to teach authorization information includes a time constraint. Denning teaches a current date and time variable which are checked against the time transmitted and password file (page 163, Login protocol using passwords).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to include a time constraint. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Denning, in order to determine the timeliness of the information.

Claim 55 and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wool and Denning 1979.

Claim 55: Wool fails to teach an instance of the application is recognized by its file location. Denning teaches files positioned in a specific location in the disk file store (Fig. 5).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to include a file's position recognition. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to access the file when needed.

Claim 62: Wool fails to teach an authorization information includes a file location. Denning teaches files positioned in a specific location in the disk file store (Fig. 5).

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system by Wool to include a file's position recognition. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so, as suggested by Levin et al., in order to access the file when needed.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Todd M Jack whose telephone number is 703-305-1027. The examiner can normally be reached on M-Th.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Albert Decady can be reached on 703-305-9595. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Todd Jack

July 25, 2004

Art Unit 2133

ALBERT DECADY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100